EXHIBIT A

LITSON.

J. Alex Little
Zachary C. Lawson
615.985.8189
alex@litson.co
zack@litson.co

May 28, 2024

VIA EMAIL

The Honorable Philip Kopczynski
Assistant United States Attorney
Office of the U.S. Attorney
for the Western District of Washington
700 Stewart Street, Suite 5220
Seattle, WA 98101
philip.kopczynski@usdoj.gov

Re: *United States v. Nevin Shetty,* 2:23-CR-84-TL
Rule 16(b)(1)(C) disclosure: Michael Perklin

Dear Counsel:

Pursuant to Federal Rule of Criminal Procedure 16(b)(1)(C), the Defendant hereby provides this notice that it intends to call Michael Perklin as a witness to provide testimony under Federal Rules of Evidence 702, 703, and 705. Mr. Perklin's qualifications are set forth in the attached curriculum vitae, which includes all publications of his in the previous ten years. Mr. Perklin has testified as an expert in the previous four years in one matter: a confidential arbitration. Mr. Perklin's opinion is provided in the attached report. While Mr. Perklin's testimony depends in large part on what the government presents in its case-in-chief, the testimony summaries and opinions below are all within Mr. Perklin's expertise.

The Defendant anticipates that Mr. Perklin will provide testimony regarding the following, as further reflected in his attached report:

1. **Background on cryptocurrency and blockchain technology.**

   It is anticipated that Mr. Perklin's testimony will describe the general structure of cryptocurrency and blockchain technology. It is anticipated that his testimony will describe the benefits of cryptocurrency and blockchain technology and how they have been integrated into major financial institutions. It is anticipated that his testimony will describe the disparity between public perception of cryptocurrency and the actual legality and legitimacy of cryptocurrency.

The basis of his opinions and testimony will be his experience as a blockchain security consultant for over 10 years.

2. **The security measures, transparency, and regulatory framework surrounding cryptocurrency.**

   It is anticipated that Mr. Perklin's testimony will describe the security measures, including by blockchains, that protect cryptocurrency. It is anticipated that Mr. Perklin's testimony will describe the transparency and traceability of cryptocurrency transactions and the logging of cryptocurrency transactions on the blockchain. It is anticipated that Mr. Perklin's testimony will describe the federal and state regulatory framework that govern cryptocurrency.

   As to this topic, Mr. Perklin will base his opinion and testimony on the same information listed in topic 1.

3. **Mr. Perklin may testify as a rebuttal witness to the government's expert testimony about any aspect of cryptocurrency and blockchain technology.**

   As to this topic, Mr. Perklin will base his opinion and testimony on the same information listed in topic 3. The Defendant will supplement a rebuttal disclosure at the appropriate time.

The Defendant reserves the right to supplement this disclosure in accordance with the Federal Rules.

Sincerely,

/s/ J. Alex Little

J. Alex Little
Zachary C. Lawson
6339 Charlotte Pike Unit C2321
Nashville, TN 37209
alex@litson.co
zack@litson.co

Jeffrey B. Coopersmith, WSBA No. 30954
1015 Second Avenue, Floor 10
Seattle, Washington 98104-1001
Ph: (206) 625-8600 | Fax: (206) 625-0900
jcoopersmith@corrcronin.com

Cryptocurrency

Legitimacy and Involvement of Institutions

If someone would only hear of cryptocurrencies via newsworthy headlines, they'd hear about the FTX fraud, the Quadriga fraud, the thefts from MTGox and Bitfinex, and conclude that the only things that happen with cryptocurrencies are frauds and thefts.

The reality is—like any technology—cryptocurrencies are completely neutral. It is up to the person who uses that technology to choose whether to use it honorably or criminally. As an example, when Grandma's purse is stolen and she loses the $100 USD inside, it would be silly to blame the USD for the acts of the thief. Unfortunately, this is precisely what less-informed individuals do when claiming "crypto is to blame" for frauds and scams.

Governments are participating in the regulation and adoption of blockchain technology. For example, on Wednesday May 22nd, 2024, the United States House of Representatives approved a bill known as FIT21, which aims to provide clarity on the regulation of blockchain technology.

Similar occurrences have occurred worldwide too, with multiple countries providing regulatory clarity on blockchain technology (Germany, Canada, Japan), and one country—El Salvador—even adopting Bitcoin as legal tender.

Benefits of Cryptocurrencies

While different investors will see different benefits in cryptocurrency, the benefits that I personally see are:

- *Uncensorable*. I have had my PayPal account frozen temporarily, I have had my bank tell me I cannot withdraw my own funds to cash, and I have had my bank refuse to send a wire transfer on my behalf despite it being my money to send to whomever I wish. A decentralized payment network allows all users to be sovereign in their financial affairs in a way that cannot be overridden by others.
- *Transparent*. The legacy financial system is opaque, meaning money paid to public goods (such as taxes, political donations, etc.) can be used improperly

with little oversight. Transparent systems like cryptocurrencies allow us to see where funds go after they're sent. This transparency makes it very difficult for bad actors to siphon funds since **everyone** can follow the money instead of only a select few accountants with access to private bank records.

- *Limited Supply*. Governments can inflate the monetary supply with the stroke of a pen, and did so with reckless abandon during recent years resulting in significant increases in the price of goods across the country. Cryptocurrencies, on the other hand, cannot have their supplies altered in the same way since there is no leader/company/administrator that controls it. Users transacting with cryptocurrencies know that the supply will not be altered.

- *Speed*. Cryptocurrencies can be transferred around the world in seconds, whereas it still can take days for wire transfers to be received. Even if the wire is "processed" within 1 day, those wired funds are often held for up to 15 days making them useless.

- *Cost*. Cryptocurrencies can be transferred around the world with fees measured in pennies, whereas wire transfers still inexplicably cost $70 to send.

- *Reversibility*. Cryptocurrency transactions are sent instantly, and become irreversible within minutes, whereas legacy financial transactions can often be reversed weeks later. When you are a merchant that just gave away your goods after receiving a credit card payment, it can be very costly to have that credit card payment reversed a month later because the cardholder decided to commit a chargeback. With cryptocurrency, your payments are yours to keep.

In regard to these benefits, cryptocurrencies are superior to legacy financial assets. They are faster, cheaper, irreversible, and cannot be censored by anyone.

The first market affected by cryptocurrency was finance with Bitcoin. It has proven particularly advantageous as a store of value despite the volatility associated with its growing pains. Bitcoin has held its purchasing power significantly better than the USD allowing holders to maintain their wealth in spite of rampant inflation.

The next market that is being disrupted with cryptocurrencies is computing with Ethereum. Instead of relying on large corporations like Amazon to host servers, users can host their applications on a decentralized blockchain where everyone can access it with significantly less fees.

I believe that—like the Internet in the 1990s—we have only just scratched the surface of the advantages this technology will bring society in the next 30 years.

Transparency and Blockchain Technology

The anonymity of cryptocurrency is one of the most prolific misconceptions about it. The reality is cryptocurrency is the most traceable form of money that has ever been invented in mankind's history. This is because all computers that participate in verifying cryptocurrency transactions store identical copies of all transactions, and compare them with each other to ensure their copies are accurate. Imagine if you had a full copy of your bank's ledgers on your computer, on your friends' computers, your family's, etc. It's impossible to hide transactions when everyone has a copy.

While each blockchain works differently, in general, when you send a unit of cryptocurrency to another account, your device (phone/computer) creates a "transaction": a small file that says "my account is transferring 123 units to that account." That transaction is then sent over the Internet to a blockchain validator. That validator then relays it to all validators it knows about, who then relay it to all validators they know about, etc. until every validator in the world has a copy. This takes only a few seconds. Once the world of validators knows about it, depending on the blockchain, the validators "write" the transaction in a way that cannot be reversed using a type of advanced cryptography.

These public blockchains make a lot of tasks easier than private banks. If there's ever any question about whether a customer did/didn't pay, either one of them can find the transaction on the public blockchain themselves to prove the payment was made without needing to request account transcripts from a middleman bank.

They also make it much more difficult for criminals to "launder" proceeds of crime since laundering requires some form of concealment. It is impossible to launder funds on a fully-transparent public blockchain since everyone can see when proceeds of crime move from one account to another.

Case Studies and Real-World Examples

On January 10, 2024, the SEC approved Bitcoin ETFs. Since then, a variety of major financial institutions have offered Bitcoin ETFs to their clients including Fidelity and Blackrock.

On May 9, 2024, Goldman Sachs and 30 other financial institutions announced the Canton network, a blockchain-based system designed to tokenize real world assets.

The world of financial transactions is changing rapidly from a collection of brick-and-mortar rooms holding pages of paperwork to a blockchain-based economy based on tokens.

Public Perception v. Reality

Humans are naturally fearful of new things. It's in our nature.

When the Internet first became used by the general public, there were a number of examples of fear for the technology. Fear of online banking, fear of misinformation on peer-sourced content like Wikipedia, fear of online predators enticing children into compromising situations, fear of hackers. It was only after people became comfortable with the new technology that they were able to set aside the fears and embrace it. I believe the same is happening now with blockchains and cryptocurrencies.

When most of the news people read about cryptocurrencies cites examples of fraud and theft, it can be natural to build an incorrect conclusion about the technology. The reality is fraudsters will use anything available to them to commit fraud: cryptocurrencies, the Internet, computers, phones, cars, dollars, gift cards, paperwork—you name it. It's important to remember that all technology is inherently neutral, and it is the person that uses the technology who chooses to use it honorably or criminally.

Knowledge is power. Understanding how to use computers and smartphones removed the fear of them, and understanding how to use cryptocurrencies is no different. The fastest way to overcome our natural fear of new things is to learn about them. When you know how it works, it is no longer a threat.

Security Measures

When it comes to frauds, there are dozens of laws and regulations that define what a fraud is, and these apply to all frauds. Committing fraud is the same whether you are Enron or FTX, using stocks or cryptocurrencies. Anyone who commits fraud can easily be held accountable, and—if anything—fraud can be much more easily proved when public transparent blockchains are involved vs private corporate records and opaque bank accounts.

As for theft, this responsibility rests squarely with the person who controls the asset. In the same way it is our responsibility to put good locks on our doors, it is our responsibility to secure the cryptocurrency we control. And if someone is offering cryptocurrency services, it is up to them to secure the cryptocurrency they control too—just like banks need to secure the dollars they hold on your behalf. There are dozens of ways to properly secure any asset, and hiring knowledgeable and experienced professionals to assist remains the recommended path for both individuals and corporations when protecting any asset from theft.

Cryptocurrency transactions are secured by blockchains which use advanced cryptography to make forgeries impossible, protecting each account from unauthorized transactions. The cryptography is so strong that every computer on the planet working together to break the encryption of a single account would not succeed before our Sun dies, taking all of humanity with it.

Just like cybersecurity standards were developed by the computing industry to help guide corporations in securing their computers and software, cryptocurrency security standards have been developed by the blockchain industry. The CryptoCurrency Security Standard (CCSS) provides a framework for businesses and individuals to assess the security of the way they work with cryptocurrencies. This framework allows people to grade the security of a system and identify which areas can be improved to increase security..

Several companies have developed novel software and novel hardware designed to make it easy to secure cryptocurrencies. Like Internet applications in the ‘90s, every new revision is easier to use by more and more people worldwide.

Market Maturity

When cryptocurrency first started trading in 2010, there were very few markets available for users to buy or sell it. It was more common to send messages to people on forums and meet them in person to trade directly.

Today there are hundreds of cryptocurrency exchanges that each offer their own order books, cryptocurrency selections, and fee structures. An analogy would be the size of a pond vs. the size of a lake. In the early days (pond), a single buy (pebble) could impact the pond greatly and cause large ripples relative to the size of the market. Today, cryptocurrency markets have grown where a single buy has negligible effect—like throwing a pebble in a lake.

There are a variety of factors that indicate that the cryptocurrency market is becoming less risky over time:

- User acquisition
- Corporate involvement
- Government laws/bills/acts that provide clarity
- Better software and hardware for interacting with cryptocurrencies
- Better education of end-users

There are far more choices of exchanges who can help buy or sell cryptocurrencies than in the early days of cryptocurrency trading. These markets have far more liquidity available on them, making larger purchases/sales easier with fewer violent price swings. Every day, using cryptocurrencies becomes easier thanks to the tireless efforts of blockchain companies around the world applying improvements and launching new products—just like the early days of the Internet.

Regulatory Framework

At this point in 2024, it would be difficult to find any developed country that has not issued some kind of laws, regulations, bills, acts, or guidance for their citizens who use cryptocurrencies. This technology is so useful that every country has addressed it in some manner. Using any new technology will always come with its own risks, so it will always be less-safe in the early days of anything when compared to a mature product. This happened with cars, electricity, computers, and the Internet before recently happening with cryptocurrency.

The general adage of "buyer beware" will always apply to everything that a "buyer" can "buy", but incremental improvements in both regulatory clarity and the technology itself will continue to make it safer for all.

On May 22nd, the House of Representatives passed the FIT21 bill which provides clarity for cryptocurrency, reducing the risks. The state of Wyoming has built a regulatory framework for various Decentralized Autonomous Organizations (DAOs) to register and gain the same legal status as corporations, allowing them the same legal protections. In El Salvador, bitcoin was adopted as legal tender, very clearly cementing its use as money in that part of the world.

All new things seem like novelties until there are legal frameworks that legitimize their use. This happened with cars, computers, and every other disruptive technology. Once there are laws/bills/acts on the books that clarify citizens' rights in

respect to this new technology, citizens can confidently use the technology knowing there is recourse for anyone's misuse of it.

Institutional Involvement

The adoption of Bitcoin ETFs in the US has allowed everyone with a 401k to allocate a portion of their portfolio to bitcoin. This outsources the control of cryptocurrency to qualified financial institutions who have the manpower and expertise in security computer systems so end-users don't have to.

I believe the risk associated with cryptocurrencies has dropped significantly as a result, paving the way for general adoption.

Blackrock, Tesla, BNY Melon, Citibank, UBS, BNP Paribas, Morgan Stanley, JP Morgan Chase, Goldman Sachs, ING… there are so many household names that have invested in cryptocurrencies. With so many "major institutions" holding one or more cryptocurrencies, at this point in 2024 it may be easier to collate a list of major institutions that have NOT invested in cryptocurrencies or blockchains in one manner or another.

Every new user and every new corporation that gets involved with cryptocurrency makes the technology and ecosystem more stable and credible. The larger the institution getting involved, the more stability/credibility the cryptocurrency market has.

Technological Innovation

There are so many technological innovations that have improved Bitcoin and cryptocurrencies since Bitcoin was launched in 2009:

- Multisignature features that require 2 or more signatures before releasing funds
- Software for devices to make it more secure to store
- Dedicated hardware so your cryptocurrency does not need to be stored on your smartphone
- Security standards to help grade and improve the security of any system controlling cryptocurrencies

- Advanced mathematics like threshold signatures and zero-knowledge-proofs that can make handling cryptocurrencies more secure while offering limited forms of privacy
- Smart contracts that provide advanced financial services without the need for banks

These security enhancements naturally reduce risks associated with cryptocurrency investments. The advanced hardware and software that has been developed drastically reduce the risks associated with cryptocurrencies, making for much safer investing. Also, the general improvement of cryptocurrency knowledge within the industry since it was formed in 2009 have improved the ecosystem as a whole in the same way as general computing knowledge improved the Internet as a whole.

DocuSigned by:
Michael Perklin
6ECCA571A725471...
Michael Perklin
May 28, 2024

Michael Perklin, *CBP, CCSSA, CISA, CISSP, EnCE, ACE*

Contact Information

Mobile: +1 (416) 992-6953
Email: mperklin@bitcoinsultants.ca
Twitter: @mperklin
LinkedIn: https://ca.linkedin.com/in/perklin

Qualifications

Michael holds the following degrees and certifications:

Master of Science in Information Assurance (MSIA), University of Davenport, Davenport, Michigan

Bachelor of Applied Information Sciences (Information Systems Security) (BaISc), Sheridan Institute, Oakville, Ontario

Computer Science Technology diploma (CST), Sheridan Institute, Oakville, Ontario

Reid Technique of Interview and Interrogation - Advanced

Certified Bitcoin Professional (CBP) #1a83e6

Certified CCSS Auditor (CCSSA) #5d3ae2

Certified Information Systems Security Professional (CISSP) #443796

Certified Information Systems Auditor (CISA) #14115468

Encase Certified Examiner (EnCE) #15-0911-4347

AccessData Certified Examiner (ACE) #UR-fc1p7132e98qw32-1229715

Affiliations

Michael is proud to be affiliated with the following organizations:

- Bitcoinsultants Inc., Principal (2012-Present)
- ShapeShift DAO, Workstream Leader (2022-Present)
- ShapeShift, Chief Information Security Officer (2017-2022)
- CryptoCurrency Certification Consortium (C4), President (2014-2021), Chairman of the Board (2021-Present)
- Rogers Communications, Lead Digital Investigator (2011-2014)
- Froese Forensic Partners / LECG (2008-2011)
- Sheridan Institute, Professor of Digital Forensics and Information Security (2012)
- Bitcoin Foundation, Director (2015-2019)
- Bitcoin Alliance of Canada, Director (2013-2016)

Relevant Experience

Michael founded Canada's first blockchain security consulting company, Bitcoinsultants, in 2012 after working in the Information-Security field for nearly a decade. Since then, he has earned an industry-wide reputation for best-in-class blockchain security consultations, and cryptocurrency security audits, and now focuses his time on Expert Witness testimony for cases related to cryptocurrencies and blockchains.

Relevant experience includes:

- Over a decade of hands-on professional experience with bitcoin, cryptocurrency and blockchain security at Bitcoinsultants Inc., the world's first blockchain security consultancy
- Served as ShapeShift's Chief Information Security Officer (CISO) from 2017-2022
- Primary author and editor of the CryptoCurrency Security Standard - a collection of security controls gleaned from the study of dozens of information systems (both breached and secured)
- Authored hundreds of reports related to digital investigations and consultations as Expert Witness
- Being deposed, cross-examined, and providing testimony as an Expert Witness in Canada, the USA, and UAE
- Lead and coordinated the world's first decentralization of an established company into a Decentralized Autonomous Organization (DAO) with ShapeShift in 2021.
- Design, implementation, and deployment of a high-security bitcoin vault system for the Ethereum crowdsale in 2014 which raised and securely stored over 30,000 BTC
- Conducted investigations into multiple high-profile breaches of cryptocurrency systems including Bitfinex and ShapeShift
- Produced the Blockchain Training Conference at multiple international locations, training lawyers, accountants, investigators and law enforcement personnel on how cryptocurrencies work (2016,2019)
- Lead a digital-forensic investigation across multiple countries that culminated in the arrest and conviction of a cryptocurrency thief in Dubai, UAE
- Software Architecture and Engineering consultation with dozens of clients designing blockchain-based information systems to ensure security and assurance of funds
- Security consultations for Initial Coin Offerings (ICOs) that launched new cryptocurrencies including Ethereum, Factom, and Zcash
- Performed source code audits of web applications to identify security vulnerabilities and misuse of cryptographic libraries
- Advised the Canadian Senate Banking Committee on bitcoin, blockchain technology and cryptocurrency investigations in 2014

Cryptocurrency and Blockchain Projects

Michael is involved in a variety of cryptocurrency related projects:

- Arkeo — A decentralized blockchain information network designed to remove central points of failure to open and public blockchain information. Michael lead the architectural design of the ShapeShift DAO's most ambitious project to replace its centralized RPC and database connections with a decentralized equivalent.
- CryptoCurrency Security Standard — The world's first formal standard for cryptocurrencies. Michael worked with industry-recognized security experts to collect and analyze information about the world's most successful and least successful cryptocurrency systems. This data was used to author the world's first standard that applies to cryptocurrencies, allowing anyone to measure a company's security practices against a common scale. Michael currently serves as the chairman of the CCSS Steering Committee.
- Certified Bitcoin Professional — The world's first personnel certification for cryptocurrencies. Michael worked with Bitcoin experts around the world to build a database of peer-reviewed exam questions for the world's first cryptocurrency certification.
- Blockchain Training Conference — The world's first blockchain conference targeted at people *outside* the blockchain industry. Michael was lead organizer of this series of training events held in countries around the world. The Blockchain Training Conference trained lawyers, accountants, developers, auditors, traders, law-enforcement personnel and anti-money-laundering specialists in how blockchains work and how work with this new technology that is sweeping the globe.
- Electrum — An open-source bitcoin wallet.
  Michael has contributed enhancements to Electrum which added a high-security feature allowing offline computers and online computers to communicate solely with QR-codes, removing the opportunity for malware to infect offline systems.

Publications

Michael has contributed the following papers to the information security community:

- Keep Bitcoin Safe by Making Security a Habit. Bitcoin Magazine, February, 2020
- "You Are What You Play": Breaching privacy and identifying users in online gaming, Transactions of the 12th Annual PST (Privacy, Security, Trust) IEEE Conference, Ryerson, Toronto, Canada, July 23-24, 2014
- Dealing with CryptoWall and Ransomware Decentral Blog, August, 2014
- Bitcoin Handbook for Non-Profits Bitcoin Foundation, October, 2014

Select Speaking Engagements

Michael has been invited to speak at more than 100 appearances worldwide. A selection of the more notable speaking engagements are listed here:

- *Everyday Opsec*
  Consensus. New York, May 2018.
- *Life in 2030*
  Blockchain Futurist. Toronto, August 2018
- *Operational Security*
  Bitcoin, Ethereum, & Blockchain Superconference, Texas, February 2018
- *Blockchain Security in 2030: A Look Forward*
  HoshoCon. Las Vegas, October 2018.
- *Blockchain Security: Past, Present, Future*
  Genesis Moscow. Moscow, September 2017
- *Thefts, Breaches, and Attacks - When Things Go Wrong*
  Blockchain:Money, London. November, 2016
- *Technology and Innovation Panel: Blockchain*
  ACAMS Canada, Toronto. Ontario, 2016
- *Blockchain Investigations*
  Blockchains, Cryptocurrencies, and AML, Toronto. August, 2016
- *The Future of Blockchains*
  Blockchain World Congress, New York. September, 2016
- *Blockchain Investigations*
  Blockchain Training Conference, Toronto. June, 2016
- *CCSS In Depth*
  Blockchain Training Conference, Toronto. June, 2016
- *Blockchains and Accounting*
  YDCPAA, Toronto. January, 2016
- *Bitcoin and Why it Matters*
  Ivey Alumni Network, Toronto. June, 2015
- *Securing Bitcoin and reaching CCSS Level III*
  Texas Bitcoin Conference, Texas. April, 2015
- *Bitcoin and Financial Technology*
  FISD Conference, New York. December, 2014
- *Bitcoin Security*
  Latin American Bitcoin Conference, Rio De Janeiro Brazil. December, 2014
- *The Bitcoin Startup Ecosystem*
  Inside Bitcoins, Las Vegas NV. October, 2014
- *Witness on Bitcoin and Cryptocurrencies Senate Committee on Banking, Trade, and Commerce*, Ottawa ON. October, 2014
- *ACL Steganography*
  Lockdown, Madison WI. June, 2014
- *High Security Bitcoin*
  Bitcoin Expo 2014, Toronto. April, 2014
- *Bitcoin - Myths and Realities.*
  Ontario Securities Commission, Toronto. February, 2014
- *The State of Cyber Security*
  FISD Conference, Toronto. November, 2013
- *Forensic Fails*
  DEF CON 21, Las Vegas. August, 2013
- *ACL Steganography*
  DEF CON 21, Las Vegas. August, 2013
- *Bitcoin 101 for Cyber Investigators*
  HTCIA Ontario Chapter, Toronto. April, 2013
- *Bitcoin for Lawyers - Up to Speed in 60m*
  [Redacted], Toronto. May, 2012
- *Anti-Forensics and Countermeasures*
  SECTOR, Toronto. October, 2012
- *Anti-Forensics and Anti-Anti-Forensics*
  DEF CON 20, Las Vegas. July, 2012
- *Defence In Depth - Don't Stop in the Middle*
  pgWest Conference, San Jose. September, 2011